

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

FILED
JAMES BONINI
CLERK

2010 AUG 19 AM 10:51

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Hewlett Packer convertible mini-tower computer, model
number 7800P, serial number MXL 82106L, black and silver
in color.

Case No.

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WESTERN DIV. DAYTON
3:10mj-197
MICHAEL R. MERZ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Hewlett Packer convertible mini-tower computer, model number 7800P, serial number MXL 82106L, black and silver in color.

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. Section
2252(a)(4)(A); and
18 U.S.C. Section
2252A(a)(5)(A).

The application is based on these facts:

Offense Description

Possession of Sexual Exploitation of Minors in Interstate
Commerce; AND Possession of Child Pornography Material of Minors in Interstate
Commerce

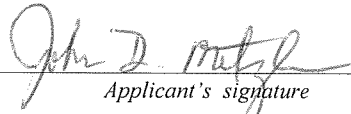
☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 08/19/2010

City and state: DAYTON, OHIO


Applicant's signature

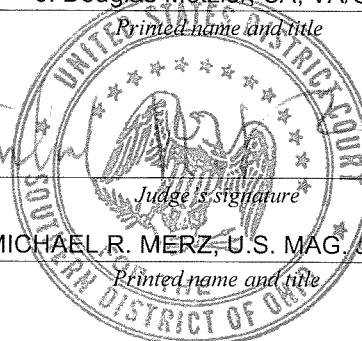
J. Douglas Metzler, SA, VA/OIG

Printed name and title


Judge's signature

MICHAEL R. MERZ, U.S. MAG. JUDGE

Printed name and title



ATTACHMENT A

The property to be searched consists of the following three electronic storage devices:

(1) Ultra thumb drive, silver and red in color; (1) Gigawire MP 3 player # 42-542 and (1)

Hewlett Packer convertible mini-tower computer, model number 7800P, serial number MXL

82106L, black and silver in color.

ATTACHMENT B

1. Electronic evidence that the computer, MP3 player, and thumb drive described in Attachment A were used as a means to commit the offenses described in the warrant, namely possessing and accessing with intent to view visual depictions involving the use of a minor in sexually explicit conduct on any land or building owned or under the control of the United States, in violation of 18 U.S.C. § 2252(a)(4)(A); and knowingly possess or access with intent to view an image of child pornography in any building owned or under the control by the United States, in violation of 18 U.S.C. § 2252A(a)(5)(A).

2. Any child pornography, whether in the form of movies, images, digital photographs, or other visual depictions of minors involved in sexual activity or sexually explicit conduct.

3. With regard to the items listed in Attachment A of this warrant:
- a. evidence of who used, owned, or controlled the items listed in Attachment A at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the items listed in Attachment A, such as viruses, Trojan horses, and other forms of malicious

software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence of the attachment of any items listed in Attachment A to other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the items in Attachment A;
- f. evidence of the times the items in Attachment A were used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the items listed in Attachment A;
- h. electronic documentation and manuals that may be necessary to access the items in Attachment A or to conduct a forensic examination of them;
- i. contextual information necessary to understand the evidence described in this Attachment B.

4. Evidence relating to the use of the Internet Protocol address to communicate, including:

- a. routers, modems, and network equipment used to connect computers to the Internet;

- b. records of Internet Protocol addresses used;
- c. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

AFFIDAVIT

I, J. DOUGLAS METZLER being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic media known as a silver and red Ultra thumb drive, a Gigawire MP3 player # 42-542 and a Hewlett Packer desktop computer serial number MXL 82106L, all described in Attachment A and hereinafter collectively referred to as “storage medium,” to search for the items particularly described in Attachment B.

2. I am a Special Agent with the United States Department of Veterans Affairs, Office of Inspector General, Criminal Investigations Division, having been so employed since May 21, 2000. I am a graduate of the Federal Law Enforcement Training Center’s Criminal Investigative Training Program, and Criminal Investigations in an Automated Environment Training Program.

3. This affidavit is based upon my direct involvement in the investigation, training, experience, conversations with law enforcement officers participating in the investigation, and consultation with persons involved in the forensic examination of computers, and is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. I, John Douglas Metzler am employed as a Special Agent with the Department of Veterans Affairs, Office of Inspector General (VA-OIG), Criminal Investigations Division. I have held this position since May 2000, and I am currently assigned to the VA-OIG office located at 1240 E. 9th Street, Rm. 1619, Cleveland, OH 44199. My duties include conducting criminal investigations relating to unlawful conduct involving property, funds or individuals on VA Medical Center (VAMC) premises.

5. On July 26, 2010, I was assigned to investigate an allegation concerning a patient at the Dayton VAMC, who allegedly was accessing child pornography using a non-VA donated computer while on VAMC premises. According to information received from the VAMC's Police Department, on Tuesday, July 20th, 2010, Officer James R. Ables was dispatched to the Bldg #410, Domiciliary, to investigate allegations of someone downloading "child pornography," on a Veteran's Industries computer. These computers are contained in a lab setting, and are for the use of resident veterans to search and apply for jobs.

6. Officer Ables met with the supervisory rehabilitation specialist, who told him that one of her "monitors" had witnessed a patient viewing child pornography on one of the computers. Officer Ables told Johnson that he needed to interview this "monitor" (the monitors are veteran patients who assign the computers as needed, monitor usage, and maintain the sign in/out log) as soon as possible. On Wednesday, July 21st, 2010 Officer Ables met with the monitor at the VAMC police office, where a tape recorded interview was conducted and subsequently transcribed.

7. The monitor stated that he saw a resident veteran, Charles E. SUTTLES (a registered sex offender), viewing child pornography on one or more of the lab's computers on various occasions over the past few weeks. The monitor told Officer Ables that SUTTLES was viewing "a bunch of pictures of naked little kids." Officer Ables asked him how young the children were, and the monitor stated "pre-teen." The monitor also said that SUTTLES always inserted a red thumb drive whenever he used a computer. The monitor believed that SUTTLES was either viewing files contained on the thumb drive, or downloading files to the thumb drive from the internet. The monitor emphasized that SUTTLES always has the thumb drive on his person. He also stated in the interview he has had no altercations with SUTTLES and only knows him casually.

8. On Thursday, July 22nd, 2010, an anonymous phone call was received at VAMC police dispatch center, stating that SUTTLES was currently in the computer lab, at the

Volunteers of America facility, Bldg #400, using the red thumb drive in one of the computers. Officer Ables went to the building #400 computer lab, where he found SUTTLES sitting at a computer typing text. A silver and red thumb drive storage device was plugged into a USB port on the computer and a Gigawire MP-3 device was plugged into another USB port, on the same computer. Officer Ables seized both devices and told SUTTLES he was under arrest for possessing child pornography. In addition, Officer Ables seized the computer that both devices were attached to which was described as a silver and black Hewlett Packer desktop computer and placed into evidence. SUTTLES was searched pursuant to arrest and transported to the VAMC police office, where he was placed in a holding cell. Suttles was later released on his own recognizance, and the items seized were placed into evidence. Affiant subsequently joined the investigation.

TECHNICAL TERMS

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

10. As described above and in Attachment B, this application seeks permission to search for electronic evidence of the above violations that might be found on the storage medium, in whatever form they are found. One form in which the evidence might be found is stored on a computer's hard drive or other storage media. Some of this electronic evidence might take the form of files, documents, and other data that is user-generated. Some of this electronic evidence, as explained below, might take a form that becomes meaningful only upon forensic analysis.

11. I submit that the computer and storage medium seized by the VAMC Police related to their investigation of SUTTLES' alleged possession of child pornography is connected to the VA monitor's observation of SUTTLES accessing child pornography using these devices. This is probable cause to believe evidence will be stored in within the items listed in Attachment A, for among the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

12. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

13. Although some of the electronic evidence sought through this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computer storage media can contain other forms of electronic evidence as well:

- a. Forensic evidence of how computers were used, the purpose of their use, who used them, and when, as described further in Attachment B, is called for by this warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal

information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team

and passed along to investigators. Whether data stored on a computer or other storage medium is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

- e. Further, in finding evidence of how the storage medium was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner. Also, the presence or absence of counter-forensic programs (and associated data) that are designed to eliminate data may be relevant to establishing the user's intent. To investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present, and, if so, whether the presence of that malicious software might explain the presence of other things found on the storage medium. I mention the possible existence of malicious software as a theoretical possibility, only; I will not know, until a forensic analysis is conducted, whether malicious software is present in this case.

14. Searching storage media for the evidence described in the attachments may require a range of data analysis techniques. It is possible that the storage media located on the

premises will contain files and information that are not called for by the warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the warrant are immediately apparent. In most cases, however, such techniques may not yield the evidence described in the warrant. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. As explained above, because the warrant calls for records of how the storage medium has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the evidence called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

15. Based upon my knowledge, training and experience, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the

accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

- a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.
- b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.
- c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or

knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.


16. In light of these concerns, I hereby request the Court's permission to seize the computer hardware, storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the items listed in Attachment A for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

17. I know that when an individual uses a computer, mp3 player, or thumb drive to view and/or obtain child pornography, the storage medium will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The storage medium is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that storage medium used to commit a crime of this type may contain electronic evidence of how the storage medium was used; data that was sent or received; evidence as to how the criminal conduct was achieved; possible records of Internet discussions about the crime; and other electronic evidence relevant to proving the commission of the crime.

CONCLUSION

18. I submit that this affidavit supports probable cause for a warrant to search the “storage medium” described in Attachment A and for the items described in Attachment B.

Affiant further sayeth naught,



J. Douglas Metzler
Special Agent
VA Office of Inspector General
Criminal Investigations Division

Subscribed and sworn to before me
on August 19, 2010:



HONORABLE MICHAEL R. MERZ
UNITED STATES MAGISTRATE JUDGE

